R E P U B L I Q U E F R A N Ç A I S E

PCT/FR03/03250

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

REC'D 04 FEB 2004
WIPO PCT

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 16 JAN. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

BEST AVAILABLE COPY

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

REQUÊTE EN DÉLIVRANCE
page 1/2

BRL

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ B / 210502

Réservé à l'INPI

REMISE DES PIÈCES
DATE 30 OCT 2002
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0213982
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 30 OCT. 2002

Vos références pour ce dossier *(facultatif)* PF020148

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

THOMSON
Karine BERTHIER
46 Quai Alphonse Le Gallo
92648 Boulogne cedex
FRANCE

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — Cochez l'une des 4 cases suivantes

Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE GESTION DE CLES SYMETRIQUES DANS UN RESEAU NUMERIQUE

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☒ Personne morale ☐ Personne physique

Nom ou dénomination sociale		THOMSON LICENSING S.A.
Prénoms		
Forme juridique		S.A.
N° SIREN		3 8 3 4 6 1 1 9 1
Code APE-NAF		3 2 2 A
Domicile ou siège	Rue	46 Quai Alphonse Le Gallo
	Code postal et ville	9 2 6 4 8 Boulogne cedex
	Pays	FRANCE
Nationalité		FRANCAISE
N° de téléphone *(facultatif)*		01 41 86 50 00 N° de télécopie *(facultatif)* 01 41 86 56 34
Adresse électronique *(facultatif)*		berthierk@thmulti.com

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 30 OCT 2002
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0213982

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		KOHRS
Prénom		Martin
Cabinet ou Société		THOMSON
N °de pouvoir permanent et/ou de lien contractuel		9016
Adresse	Rue	46 Quai Alphonse Le Gallo
	Code postal et ville	9 2 6 4 8 Boulogne cedex
	Pays	FRANCE
N° de téléphone *(facultatif)*		01 41 86 52 73
N° de télécopie *(facultatif)*		01 41 86 56 34
Adresse électronique *(facultatif)*		kohrsm@thmulti.com
7 INVENTEUR (S)		Les inventeurs sont nécessairement des personnes physiques
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☒ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : AG
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)	VISA DE LA PRÉFECTURE OU DE L'INPI
Martin KOHRS Mandataire	

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention se rapporte d'une manière générale au domaine de la gestion de clés cryptographiques dans des réseaux numériques locaux et plus particulièrement dans des réseaux numériques domestiques.

Un tel réseau est constitué d'un ensemble de dispositifs reliés entre eux par un bus numérique, par exemple un bus selon la norme IEEE 1394. Il comprend notamment deux types de dispositifs :

- Des dispositifs sources capables d'émettre des données sur le réseau : Ces dispositifs peuvent récupérer les données à travers un « canal » externe au réseau.

- Des dispositifs de présentation, adaptés à recevoir les données circulant sur le réseau, pour les traiter ou les présenter à l'utilisateur.

Ainsi, si on prend l'exemple d'un réseau numérique domestique destiné à véhiculer des données audio et/ou vidéo dans différentes pièces d'une maison, les dispositifs sources sont par exemple des décodeurs numériques recevant des programmes vidéo de l'extérieur du réseau, via une antenne satellite ou via une connexion au câble, ou bien des lecteurs de disques optiques diffusant sur le réseau, sous forme numérique, des données (audio et/ou vidéo) lues sur un disque (le disque contient dans ce cas des données provenant de l'extérieur du réseau). Les dispositifs de présentation sont par exemple des récepteurs de télévision permettant de visualiser des programmes vidéo reçus du réseau ou, d'une manière plus générale tout type d'appareil ayant la capacité de déchiffrer des données chiffrées.

Si on se place du point de vue des fournisseurs de contenu qui fournissent les données en provenance de l'extérieur du réseau local, notamment des prestataires de services diffusant des programmes télévisés payants ou bien des éditeurs de disques optiques par exemple, il est nécessaire d'éviter que ces données transmises ne soient copiées et puissent circuler facilement (par exemple en étant copiées sur un disque optique ou tout autre support d'enregistrement) d'un réseau local à l'autre.

Pour cela, il est connu de transmettre les données sous forme secrète en les chiffrant à l'aide d'algorithmes de cryptographie utilisant des clés qui sont connues au préalable des appareils autorisés à recevoir ces données ou bien qui sont échangées selon des protocoles particuliers sécurisés entre le fournisseur de contenu et ces appareils.

La demande de brevet PCT WO 00/62505 au nom de THOMSON multimédia, déposée le 31 mars 2000 et revendiquant la priorité d'une demande

de brevet française au nom du même demandeur, déposée le 13 avril 1999 et publiée sous la référence FR 2792482, concerne un réseau domestique dans lequel une clé publique propre au réseau est utilisée pour chiffrer les données circulant entre des appareils du réseau, typiquement des dispositifs sources précédemment mentionnés vers des dispositifs de présentation. Seuls les appareils de ce réseau possèdent la clé privée correspondant à la clé publique. Le couple (clé publique, clé privée) étant spécifique au réseau, des données chiffrées dans le cadre de ce réseau ne peuvent être déchiffrées par des appareils d'un autre réseau.

L'utilisation d'un couple de clés asymétriques présente certains avantages, mais aussi quelques inconvénients. Un des principaux avantages est qu'aucun secret n'est mémorisé dans les appareils sources: ces appareils ont connaissance de la clé publique, mais non de la clé privée. Cependant, la mise en œuvre de clés asymétriques est d'une relative lenteur, par rapport à celle de clés symétriques. De plus, la durée de vie de clés asymétriques est faible, exigeant une révocation périodique et la création de nouvelles clés. Dans ce cas, des données chiffrées avec une clé, puis enregistrées, pourraient soudainement ne plus être déchiffrables sur le réseau. De plus, un nombre important de paires de clés asymétriques est nécessaire.

On serait alors tenté par la mise en oeuvre d'une clé symétrique pour chiffrer les données. Or, cela exigerait que les dispositifs source aient connaissance de cette clé, ce qui leur imposerait des contraintes de sécurité accrues et les rendrait par conséquent plus onéreux.

La présente invention vise à résoudre les problèmes précités.

L'invention a pour objet un procédé de gestion de clé symétrique dans un réseau de communication consistant à obtenir dans un dispositif d'un premier type contenant :

- une première clé de chiffrement symétrique et
- ladite première clé symétrique chiffrée avec une seconde clé symétrique de réseau connue seulement d'un dispositif d'un second type raccordé audit réseau ;

une nouvelle clé de chiffrement symétrique chiffrée par ladite seconde clé symétrique

procédé dans lequel la communication entre le dispositif d'un premier type et le dispositif d'un second type est sécurisée grâce à la première clé symétrique (K_C).

Les caractéristiques et avantages de l'invention apparaîtront à travers la description d'exemples de réalisation particuliers non limitatifs, explicité à l'aide des figures jointes, parmi lesquelles :

- la figure 1 est un schéma bloc d'un réseau de communication reliant plusieurs appareils dans lequel est mise en œuvre l'invention;
- les figures 2 à 5 sont des diagrammes temporels illustrant les communications entre un dispositif source de données chiffrées et un dispositif de présentation desdites données dans un tel réseau selon différents modes de réalisation de l'invention.

On décrira dans un premier temps un exemple de réseau de communication pour illustrer la façon dont les données et les clés diverses sont échangées. Par la suite, on décrira de manière plus détaillée la gestion proprement dite des clés et leur utilisation pour une transmission de données sécurisé entre un dispositif source et un dispositif de présentation.

I] Description du réseau

Sur la figure 1, on a représenté un réseau numérique domestique comprenant un dispositif source 1, un dispositif de présentation 2 et un dispositif d'enregistrement 3 reliés ensembles par un bus numérique 4, qui est par exemple un bus selon la norme IEEE 1394.

Le dispositif source 1 comprend un décodeur numérique 10 doté d'un lecteur de carte à puce muni d'une carte à puce 11. Ce décodeur reçoit des données numériques, notamment des programmes audio/vidéo distribués par un prestataire de service.

Le dispositif de présentation 2 comprend un récepteur de télévision numérique (DTV) 20 doté d'un lecteur de carte à puce muni d'une carte à puce 21 et le dispositif d'enregistrement 3 est notamment un magnétoscope numérique (DVCR).

Les données numériques qui entrent sur le réseau via le dispositif source 1 sont en général des données embrouillées par un fournisseur de contenu, par exemple selon le principe de la télévision payante. Dans ce cas, les données sont embrouillées à l'aide de mots de contrôle CW (de l'anglais « Control Word ») qui sont eux-mêmes transmis dans le flux de données sous forme chiffrée à l'aide d'une clé de chiffrement K_F en étant contenus dans des

messages de contrôle ECM (de l'anglais « Entitlement Control Message »). La clé de chiffrement K_F est mise à la disposition des utilisateurs qui ont payé pour recevoir les données, notamment en étant stockée dans une carte à puce. Dans l'exemple de la figure 1, la carte à puce 11 contient une telle clé K_F ainsi qu'un module d'accès conditionnel CA 14 capable de déchiffrer les mots de contrôle CW.

On notera cependant que bien souvent, l'autorisation de recevoir les données n'est que temporaire, tant que l'utilisateur paie un abonnement au fournisseur de contenu. La clé K_F est donc modifiée régulièrement par le fournisseur de contenu. Grâce au procédé qui sera décrit ci-dessous, l'utilisateur pourra néanmoins enregistrer des programmes transmis pendant qu'il est abonné et les relire autant de fois qu'il le souhaite sur son propre réseau, même lorsque la clé K_F aura été changée. Par contre, comme les données sont enregistrées sous forme embrouillée de la manière décrite, elles ne pourront être relues que sur le réseau de l'utilisateur qui les a enregistrées.

Le dispositif source 1 qui reçoit ces données numériques embrouillées les met ensuite en forme pour qu'elles soient diffusées sur le réseau numérique selon un format de protection spécifique au réseau domestique. Le décodeur 10 comporte un module « unité ECM » 13 qui extrait du flux de données reçu les messages ECM contenant les mots de contrôle chiffrés à l'aide de la clé K_F pour les transmettre au module CA 14. Celui-ci déchiffre les mots de contrôle CW et les transmet à un module convertisseur 12 également contenu dans la carte à puce 11.

Le module convertisseur 12 contient une clé symétrique K_C dont la génération et la transmission entre les appareils du réseau seront décrites ultérieurement.

On notera que sur la figure 1, le réseau est représenté dans l'état dans lequel il se trouve lorsque tous les appareils ont été raccordés et ont échangé des clés cryptographiques selon des procédés qui seront décrits ultérieurement. La figure 1 illustre en particulier, pour le dispositif source 1 et le dispositif de présentation 2, toutes les clés contenues dans chaque dispositif. Les clés représentées ne sont pas forcément présentes à tout moment dans les dispositifs.

En particulier, le dispositif de présentation 2 comporte dans une mémoire une clé symétrique de réseau K_N. Cette clé est distribuée à tout nouveau dispositif de présentation nouvellement connecté au réseau selon un procédé sécurisé qui ne fait pas l'objet de la présente invention et ne sera pas

décrit davantage. De plus, chaque dispositif de présentation possède une paire de clés asymétriques (K_{PUBT}, K_{PRIT}), la première clé étant privée et la seconde publique. Ces clés sont utilisées dans le cadre de l'authentification des appareils du réseau, ainsi que pour l'échange initial des clés symétriques comme on le verra ultérieurement.

Le module convertisseur 12 utilise la clé symétrique K_C pour chiffrer les mots de contrôle CW et il insère ces mots de contrôle chiffrés dans des messages notés LECM (de l'anglais « Local Entitlement Control Message »). Ces messages LECM ont la même fonction que les messages ECM inclus dans le flux de données reçus initialement, à savoir transmettre les mots de contrôle sous une forme protégée, mais dans les messages LECM, les mots de contrôle CW y sont chiffrés à l'aide de la clé symétrique K_C au lieu d'être chiffrés à l'aide de la clé K_F du fournisseur de contenu.

De préférence, la clé K_C est fréquemment renouvelée, par exemple lors de l'initiation de chaque transmission de données, dans le but d'éviter que le dispositif source ne comporte un secret à long terme, qui exigerait une protection renforcée.

Le module convertisseur 12 insère en outre dans les messages LECM la clé symétrique K_C elle même, mais chiffrée à l'aide d'une autre clé symétrique K_N par un algorithme E2, c'est à dire $E2\{K_N\}(K_C)$.

Dans le reste de la description, on utilisera toujours la notation « E{K}(M) » pour signifier chiffrement de données M par un algorithme E avec une clé K.

La clé K_N, que nous appellerons dans la suite clé de réseau, ne réside pas dans l'appareil source 1, mais dans l'appareil de présentation 2. Suite à la création de la clé K_C, cette dernière est transmise de manière sécurisée à l'appareil de présentation 2, qui la chiffre à l'aide de K_N et retransmet le résultat à l'appareil source qui le mémorise dans le module convertisseur 12 de sa carte, pour utilisation ultérieure.

Les messages LECM ainsi construits sont ensuite transmis à l'unité ECM 13 qui les insère dans le flux de données à la place des messages ECM. Il est à noter que lorsque le contenu reçu n'est pas déjà sous forme embrouillée comme décrit ci-dessus et ne contient pas de message ECM, le module convertisseur 12 est chargé dans ce cas de mettre les données sous cette forme pour que le flux de données diffusé sur le bus 4 soit toujours sous la forme de paquets de données tels le paquet 40 représenté à la figure 1 contenant un message LECM et des données embrouillées.

On peut résumer le contenu de ce paquet comme suit :
LECM | E4{CW}(<données>) ; soit :
E2{K_N}(KC) | E3{K_C}(CW) | E4{CW}(<données>) ;
où « | » représente l'opérateur de concaténation.

Les données circulent donc toujours sous forme chiffrée dans le bus 4, et seuls les appareils ayant accès à la clé symétrique K_C sont capables de déchiffrer les mots de contrôles CW et donc de déchiffrer les données. Ces appareils sont ceux possédant la clé de réseau K_N. Ceci empêche donc la diffusion vers d'autres réseaux locaux de toute copie effectuée dans le réseau domestique de la figure 1.

Lorsque les paquets de données 40 sont reçus par le récepteur de télévision numérique 20, ils sont transmis au module « Unité LECM » 23 qui en extrait les messages LECM pour les transmettre à un module terminal 22 contenu dans la carte à puce 21. Ce dernier déchiffre tout d'abord E2{K_N}(K_C) à l'aide de la clé K_N qu'il contient pour obtenir la clé K_C. Ensuite, à l'aide de la clé K_C, il déchiffre E3{K_C}(CW) pour obtenir le mot de contrôle CW qu'il transmet au module « Unité LECM » 23. Celui-ci est alors en mesure de désembrouiller les données E4{CW}(<données>) à l'aide du mot de contrôle. Les données désembrouillées sont ensuite présentées à l'utilisateur. Dans le cas de données vidéo, celles-ci peuvent être visualisées sur le récepteur de télévision 20.

Grâce au réseau numérique local qui vient d'être décrit, le flux de données numériques reçu d'un fournisseur de contenu est transformé par le dispositif source qui le reçoit en un flux de données dans lequel les données (ou plus précisément les mots de contrôle CW) sont chiffrées avec à une clé symétrique K_C. La clé K_C est transmise avec les données chiffrées avec son aide, en étant elle-même chiffrée à l'aide d'une autre clé symétrique, la clé de réseau K_N. Le flux de données qui circule dans le réseau local contient ainsi des données ayant un format spécifique à ce réseau local qui ne peuvent être déchiffrées que par les dispositifs de présentation du réseau local qui contiennent tous la clé du réseau K_N.

De plus, comme la clé K_C est diffusée avec les données (sous forme chiffrée), elle peut être enregistrée, par exemple par le magnétoscope numérique (DVCR) 4, en même temps que les données ce qui permettra un accès ultérieur aux données chiffrées.

Par ailleurs, comme la clé de réseau K_N n'est pas stockée dans les dispositifs sources, ceux-ci ne contiennent donc pas de secret « long terme », exigeant des précautions de sécurité accrues.

La clé K_C doit cependant être renouvelée fréquemment et nous allons maintenant décrire plus précisément comment cette clé K_C est générée et comment son chiffrement à l'aide de la clé de réseau K_N est obtenu selon différentes variantes.

II] Génération et gestion de la clé symétrique K_C lors d'une première connexion au réseau d'un dispositif source

Supposons que le dispositif source 1 vient juste d'être connecté au réseau domestique illustré à la figure 1. Il ne possède au départ aucune clé dans son module convertisseur 12.

Le figure 2 illustre les étapes d'un protocole initial permettant au dispositif source d'obtenir une clé symétrique K_C chiffrée à l'aide de la clé de réseau K_N détenue par un dispositif de présentation du réseau.

Lors d'une première étape 101, le dispositif source 1 lance une requête sur le réseau, demandant à tout dispositif de présentation de lui transmettre sa clé publique. Sur la figure 1, nous avons représenté un seul dispositif de présentation mais naturellement, le réseau numérique domestique peut comporter plusieurs dispositifs de présentation différents raccordés au bus 4. Tous les dispositifs de présentation présents et en état « d'éveil » sur le réseau (c'est à dire ceux dont l'alimentation n'est pas coupée ou bien qui ne sont pas dans un mode de mise en veille avec une alimentation très réduite des circuits du dispositif) sont supposés répondre à la requête du dispositif source en renvoyant leur clé publique

Nous supposerons dans la suite que la première clé reçue par le dispositif source 1 est la clé publique K_{PUBT} envoyée au cours de l'étape 102 par le dispositif de présentation 2. Le dispositif source 1 prend en compte le premier message reçu et échangera ensuite des messages avec le dispositif de présentation correspondant.

Le dispositif source 1, et plus précisément le module convertisseur 12, génère ensuite de manière aléatoire une clé symétrique « court terme » K_C et il mémorise cette clé K_C (étape 103). Il utilise par exemple pour la génération de K_C un générateur de nombre pseudo-aléatoire.

La clé K_C est ensuite chiffrée à l'étape 104 avec la clé publique K_{PUBT} par l'intermédiaire d'un algorithme de chiffrement asymétrique E1, par exemple l'algorithme « RSA OAEP » (pour « Rivest, Shamir, Adleman Optimal Asymmetric Encryption Padding » – décrit dans « *PKCS#1: RSA Cryptography*

Specifications, version 2.0 (October 1998) »), puis transmise sous forme chiffrée $E1\{K_{PUBT}\}(K_C)$ au dispositif de présentation 2 (étape 105). Ce dernier déchiffre la clé K_C à l'aide se sa clé privée KPRIT puis il la chiffre de nouveau selon un algorithme de chiffrement symétrique E2 à l'aide de la clé symétrique de réseau K_N (étape 106) et renvoie K_C ainsi chiffrée (i.e. $E2\{K_N\}(K_C)$) au dispositif source (étape 107), qui mémorise cette information (étape 108), de préférence dans son module convertisseur 12.

A l'issu de cette première série d'étapes 101 à 108, le dispositif source 1 possède donc dans son module convertisseur 12, une clé symétrique K_C qui va pouvoir être utilisée pour chiffrer des données, typiquement des mots de contrôles CW, et le chiffrement de cette clé K_C à l'aide de la clé de réseau K_N. Il est donc prêt à diffuser des données sur le réseau. On notera que le dispositif source ne connaît pas la clé secrète de réseau K_N.

Les étapes ultérieures 109 à 113 illustrées à la figure 2 concernent la transmission de données « utiles », c'est à dire typiquement des données audio vidéo embrouillées.

Les données reçues par le dispositif source 1 comportent des messages ECM. Le dispositif source déchiffre ces derniers pour en extraire les mots de contrôle CW puis il chiffre les mots de contrôle CW à l'aide de la clé symétrique K_C par l'intermédiaire d'un algorithme de chiffrement symétrique E3 (étape 109). Le dispositif source 1 réinsère ensuite ces mots de contrôle chiffrés (i.e. $E3\{K_C\}(CW)$) dans le flux de données et transmet l'ensemble sur le bus 4 à destination du ou des dispositifs de présentation présents sur le réseau (étape 110). Le dispositif source envoie également lors de l'étape 110 la clé K_C chiffrée à l'aide de K_N qu'il avait précédemment mémorisée à l'étape 108. En pratique, les données $E2\{K_N\}(K_C)$ et $E3\{K_C\}(CW)$ sont insérées dans le message LECM qui est transmis avec les données « utiles » embrouillées E4{CW}(<Données>).

On notera également que les données utiles transmises à l'étape 110 sont chiffrées selon un algorithme de chiffrement symétrique E4 à l'aide des mots de contrôle CW.

Le dispositif de présentation 2 qui reçoit les données transmises à l'étape 110 déchiffre tout d'abord $E2\{K_N\}(K_C)$ à l'aide de K_N pour obtenir la clé K_C qui est mémorisée (étape 111) et, à l'aide de K_C, il peut déchiffrer $E3\{K_C\}(CW)$ pour accéder aux mots de contrôle CW (étape 112) et ainsi désembrouiller les données utiles (étape 113).

Les algorithmes de chiffrement symétriques E2, E3 et E4 peuvent être identiques ou différents. On pourra utiliser par exemple l'algorithme « AES » (pour « Advanced Encryption Standard » – aussi appelé « Rijndael » – et décrit par J. Daemen et V. Rijmen dans « *Proceedings from the First Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (NIST), août 1998* »), ou encore l'algorithme « TwoFish » (décrit dans l'article « *TwoFish – a Block Encryption Algorithm* » de B. Schneier, J. Kelsey, D. Whiting, D. Wagner, N. Ferguson et publié dans le même rapport de conférence NIST).

III] Renouvellement de la clé symétrique K_C

Lorsqu'il est nécessaire de renouveler la clé K_C, notamment avant de diffuser un nouveau contenu numérique sur le réseau, on pourrait envisager d'utiliser le même protocole que celui décrit à la figure 2 (étapes 101 à 108). Néanmoins, ce protocole implique des calculs de chiffrement utilisant des algorithmes asymétriques qui exigent une puissance de calcul assez importante et qui sont relativement long à mettre en œuvre dans des processeurs de carte à puce. C'est pourquoi, pour le renouvellement de la symétrique « court terme » K_C, un second protocole est utilisé.

La figure 3 illustre un premier mode de réalisation de ce second protocole permettant le renouvellement de la clé symétrique K_C.

A l'étape 200, le dispositif source 1 (ou plus précisément son module convertisseur 12) génère de manière aléatoire une nouvelle clé symétrique K'_C de la même façon qu'a été générée la clé K_C à l'étape 103 puis il mémorise K'_C.

A l'étape suivante 201, le dispositif source chiffre la nouvelle clé K'_C à l'aide de la clé K_C précédente en utilisant un algorithme de chiffrement symétrique E5 puis il diffuse sur le réseau (étape 202) le résultat de ce chiffrement $E5\{K_C\}(K'_C)$ accompagné de la clé K_C elle-même chiffrée par la clé du réseau K_N ($E2\{K_N\}(K_C)$). Cette valeur $E2\{K_N\}(K_C)$ avait en effet été mémorisée à l'issu du premier protocole à l'étape 108.

Tout dispositif de présentation raccordé au réseau et en état « d'éveil » reçoit les données diffusées à l'étape 202 et il les traite conformément aux étapes 203 à 206. Nous supposons ici que le dispositif de présentation 2 est le premier dispositif de présentation qui répond au message diffusé par le dispositif source à l'étape 202.

Le dispositif de présentation (ou plus précisément son module terminal 22) déchiffre tout d'abord $E2\{K_N\}(K_C)$ avec la clé K_N (étape 203), puis ayant récupéré la clé K_C, il déchiffre $E5\{K_C\}(K'_C)$ avec K_C pour obtenir K'_C (étape 204). Il chiffre ensuite la nouvelle clé K'_C avec la clé de réseau K_N (étape 205) avant de renvoyer le résultat de ce chiffrement $E2\{K_N\}(K'_C)$ au dispositif source 1 (étape 206). Le dispositif source remplace alors à l'étape 207 les valeurs de K_C et $E2\{K_N\}(K_C)$ mémorisées dans son module convertisseur 12 par les valeurs correspondant à la nouvelle clé : K'_C et $E2\{K_N\}(K'_C)$.

On constate donc que pour obtenir une nouvelle clé symétrique K'_C et son chiffrement à l'aide de la clé de réseau K_N, il n'a été nécessaire, selon le protocole décrit, d'effectuer que deux échanges de données (étapes 202 et 206) entre le dispositif source et un dispositif de présentation. De plus, seuls des algorithmes de chiffrement symétrique sont utilisés dans ce protocole de renouvellement de clé ce qui allège les charges de calcul pour les processeurs situés dans les cartes à puces des dispositifs, en particulier pour celui du dispositif source1.

On notera qu'après ce renouvellement de clé, des données « utiles » peuvent être diffusées par le dispositif source 1 de la même manière que précédemment à l'étape 110. L'étape 208 de la figure 3 illustre cette diffusion de données utilisant la nouvelle clé K'_C à la place de la clé K_C. Ces données sont exploitées par le dispositif de présentation 2 de la même manière qu'aux étapes 111 à 113 de la figure 2.

La figure 4 illustre une variante de ce mode de réalisation permettant le renouvellement de la clé symétrique K_C.

Les étapes 300 à 304 sont identiques aux étapes 200 à 204 du protocole de la figure 3 qui ont déjà été décrites.

A l'étape 305, au lieu de chiffrer directement la clé K'_C obtenue à l'étape 304, le dispositif de présentation 2 (ou plus précisément son module terminal 22) calcule un nouveau nombre X en appliquant une fonction connue aux clés K_C et K'_C. De manière préférentielle, la fonction utilisée est la fonction XOR et on effectue à l'étape 305 : $X = K_C \text{ XOR } K'_C$.

Les étapes 306 et 307 sont similaires aux étapes 205 et 206 du protocole de la figure 3 sauf que le dispositif de présentation 2 chiffre le nombre X et non la clé K'_C à l'aide de la clé de réseau K_N.

Lorsque le dispositif source reçoit le message envoyé à l'étape 307, il effectue à l'étape 308 le calcul du nombre X à partir des clés K_C et K'_C en

utilisant la même fonction qu'à l'étape 305. Ce calcul de X peut également être effectué auparavant à tout moment après la génération de la nouvelle clé K'_C.

Le nombre X ainsi calculé et la valeur de son chiffrement à l'aide de la clé de réseau K_N ($E2\{K_N\}(X)$) sont ensuite mémorisés (étape 309) par le module convertisseur 12 du dispositif source 1 à la place de la clé symétrique K_C précédente et de son chiffrement à l'aide de la clé de réseau ($E2\{K_N\}(K_C)$).

A l'étape 310, qui n'est pas nécessairement exécutée juste après l'étape 309, nous avons illustré la manière dont sont diffusées les données « utiles » par le dispositif source 1 en utilisant la nouvelle clé symétrique X.

La figure 5 illustre un second mode de réalisation du second protocole permettant le renouvellement de la clé symétrique K_C.

Selon ce mode de réalisation, lors d'une première étape 400, le dispositif source 1 (ou plus précisément son module convertisseur 12) génère un nombre aléatoire D et il le mémorise. Il calcule ensuite (étape 401) la nouvelle clé symétrique K'_C en appliquant une fonction f à la clé K_C mémorisée lors du premier protocole (à l'étape 103) et au nombre D. Le fonction f est notamment une fonction de dérivation classique telle qu'une fonction de hachage (on peut par exemple utiliser la fonction SHA-1 décrite dans le document « *Secure Hash Standard, FIPS PUB 180-1, National Institute of Standard Technology, 1995* ») ou bien encore une fonction de cryptage telle que la fonction XOR.

L'étape 402 correspond à l'étape 109 du protocole de la figure 2 et consiste à extraire les messages ECM inclus dans les données reçues par le dispositif source pour les déchiffrer dans le module CA 14 et en extraire les mots de contrôle CW qui sont ensuite chiffrés dans le module convertisseur en utilisant la nouvelle clé symétrique K'_C. Par contre la diffusion des données « utiles » sur le réseau par le dispositif source est un peu différente de celle effectuée à l'étape 110.

En effet, à l'étape 403, le dispositif source insère dans le message LECM la donnée D générée à l'étape 400. Il insère en outre dans ce message LECM :

- la clé symétrique K_C initiale chiffrée avec la clé du réseau K_N ($E2\{K_N\}(K_C)$) et
- un ou des mots de contrôle CW chiffré(s) avec la nouvelle clé symétrique K'_C ($E3\{K'_C\}(CW)$).

Lorsque le dispositif de présentation 2 reçoit les données diffusées à l'étape 403, il déchiffre tout d'abord $E2\{K_N\}(K_C)$ avec la clé du réseau K_N (étape 404), puis il calcule la nouvelle clé symétrique K'_C à partir de K_C et de D en appliquant la fonction f (étape 405). Ayant obtenu K'_C, il peut ensuite déchiffrer $E3\{K'_C\}(CW)$ pour obtenir le mot de contrôle CW (étape 406) et désembrouiller les données « utiles » à l'aide de ce mot de contrôle (étape 407).

Grâce à ce mode de réalisation, il n'est pas nécessaire d'effectuer un échange de données entre un dispositif source et un dispositif récepteur pour obtenir le renouvellement d'une clé symétrique K'_C. Ceci est particulièrement avantageux par exemple lorsque aucun dispositif de présentation n'est en état « d'éveil » dans le réseau et qu'un utilisateur souhaite enregistrer un programme (contenu numérique) reçu par le dispositif source. Le dispositif source pourra ainsi renouveler sa clé de chiffrement symétrique K_C sans avoir besoin d'un quelconque dispositif de présentation et pourra donc diffuser des données utiles accompagnées de messages LECM protégés par cette clé renouvelée pour que les données soient enregistrées dans une unité de stockage numérique telle que le magnétoscope 3 de la figure 1.

REVENDICATIONS

1. Procédé de gestion de clé symétrique dans un réseau de communication consistant à obtenir dans un dispositif d'un premier type contenant :

- une première clé de chiffrement symétrique (K_C) et
- ladite première clé symétrique (K_C) chiffrée ($E2\{K_N\}(K_C)$) avec une seconde clé symétrique de réseau (K_N) connue seulement d'un dispositif d'un second type raccordé audit réseau ;

une nouvelle clé de chiffrement symétrique (K'_C) chiffrée par ladite seconde clé symétrique (K_N)

procédé dans lequel la communication entre le dispositif d'un premier type et le dispositif d'un second type est sécurisée grâce à la première clé symétrique (K_C).

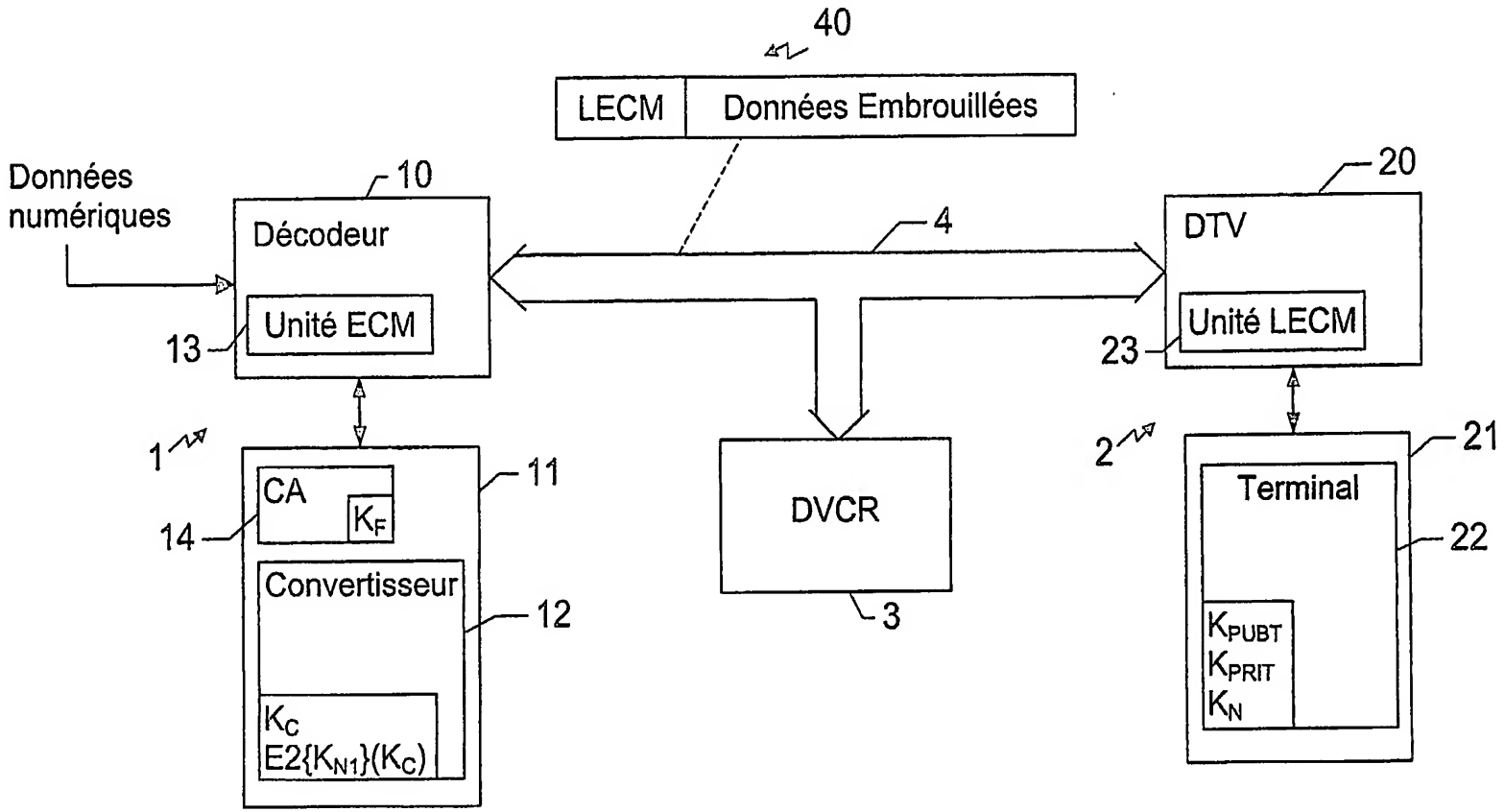

40
LECM
Données Embrouillées
Données numériques
10
Décodeur
Unité ECM
13
4
20
DTV
Unité LECM
23
1
CA
K_F
14
11
Convertisseur
12
K_C
$E2\{K_{N1}\}(K_C)$
DVCR
3
2
21
Terminal
22
K_{PUBT}
K_{PRIT}
K_N

Fig. 1

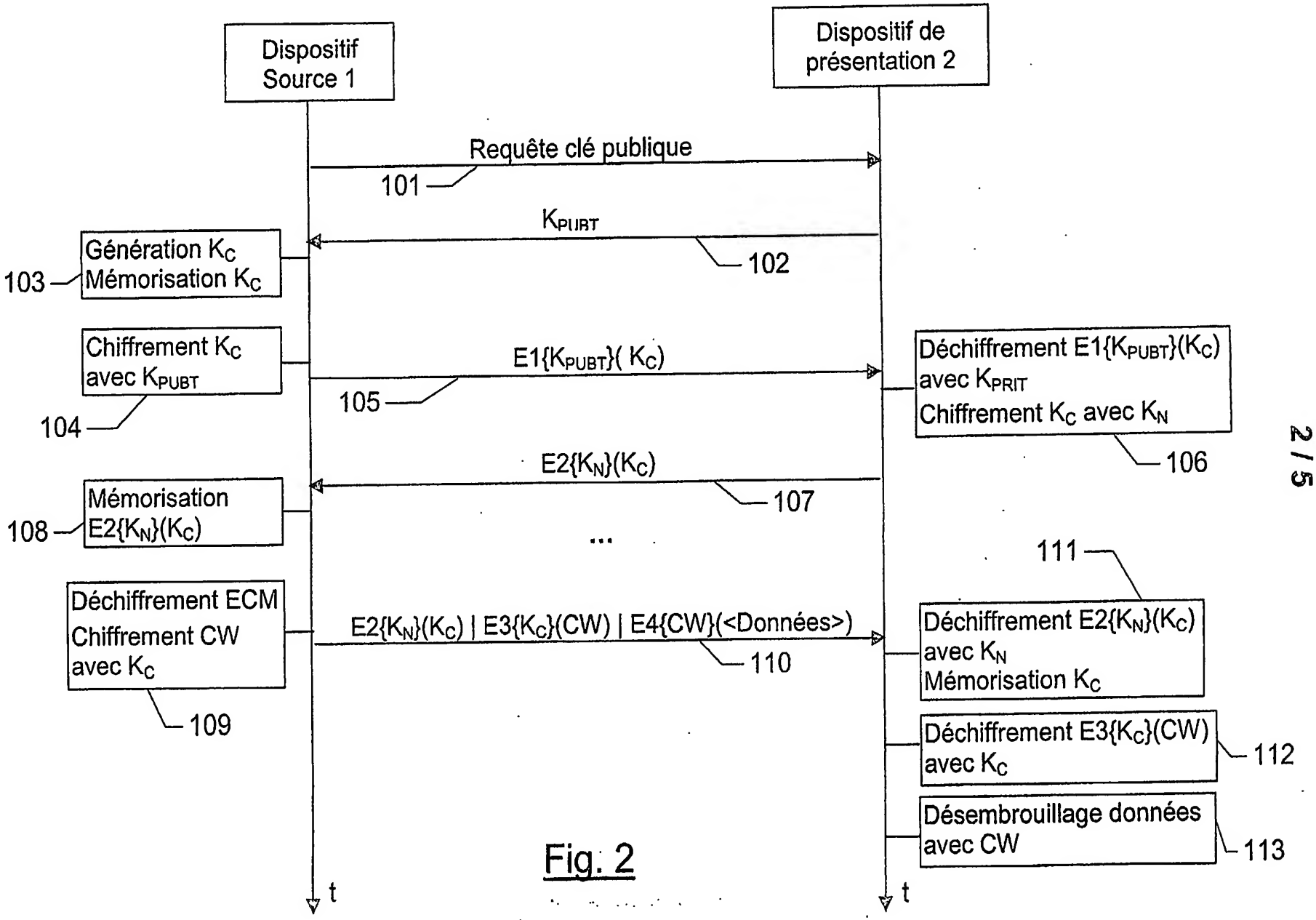

Dispositif Source 1
Dispositif de présentation 2
Requête clé publique
101
K_{PUBT}
102
Génération K_C
Mémorisation K_C
103
Chiffrement K_C avec K_{PUBT}
104
$E1\{K_{PUBT}\}(K_C)$
105
Déchiffrement $E1\{K_{PUBT}\}(K_C)$ avec K_{PRIT}
Chiffrement K_C avec K_N
106
$E2\{K_N\}(K_C)$
107
Mémorisation $E2\{K_N\}(K_C)$
108
...
111
Déchiffrement ECM
Chiffrement CW avec K_C
109
$E2\{K_N\}(K_C) \mid E3\{K_C\}(CW) \mid E4\{CW\}(<Données>)$
110
Déchiffrement $E2\{K_N\}(K_C)$ avec K_N
Mémorisation K_C
Déchiffrement $E3\{K_C\}(CW)$ avec K_C
112
Désembrouillage données avec CW
113
t
t

Fig. 2

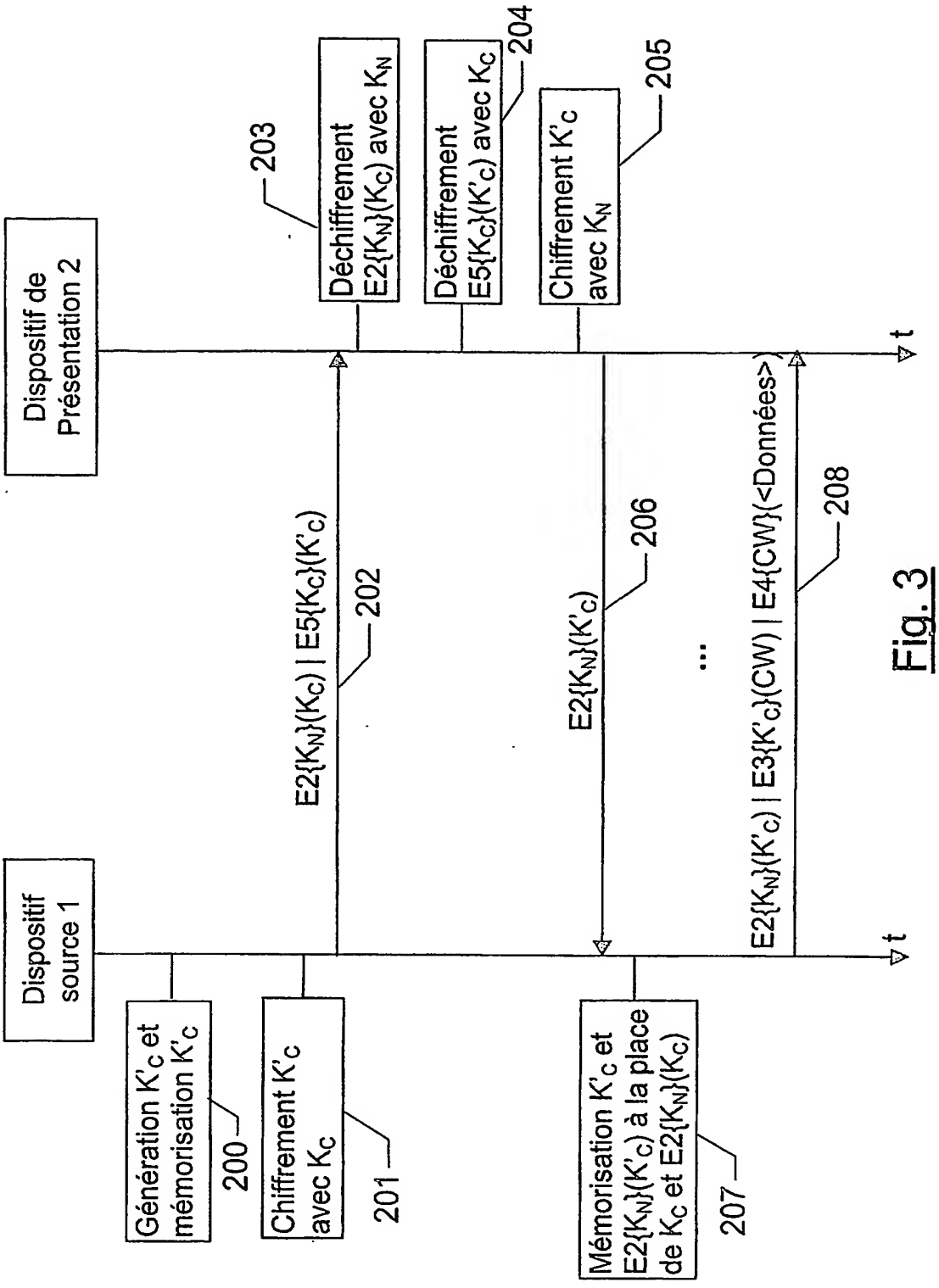

Dispositif source 1
Dispositif de Présentation 2
Génération K'c et mémorisation K'c
200
Chiffrement K'c avec Kc
201
E2{KN}(Kc) | E5{Kc}(K'c)
202
Déchiffrement E2{KN}(Kc) avec KN
203
Déchiffrement E5{Kc}(K'c) avec Kc
204
Chiffrement K'c avec KN
205
E2{KN}(K'c)
206
Mémorisation K'c et E2{KN}(K'c) à la place de Kc et E2{KN}(Kc)
207
E2{KN}(K'c) | E3{K'c}(CW) | E4{CW}(<Données>
208
t
t

Fig. 3

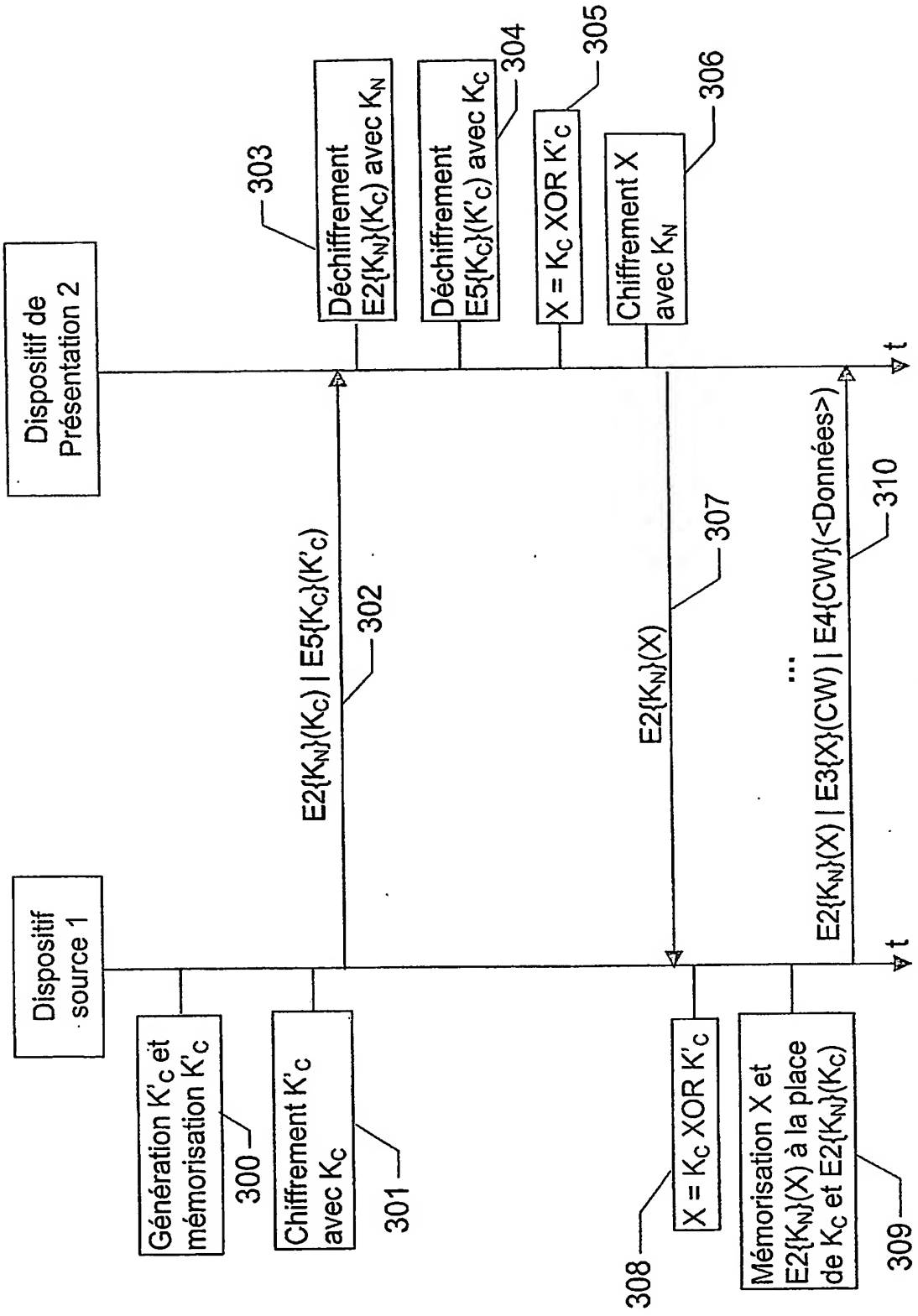

Dispositif source 1
Dispositif de Présentation 2
Génération K'c et mémorisation K'c
300
Chiffrement K'c avec Kc
301
E2{KN}(Kc) | E5{Kc}(K'c)
302
Déchiffrement E2{KN}(Kc) avec KN
303
Déchiffrement E5{Kc}(K'c) avec Kc
304
X = Kc XOR K'c
305
Chiffrement X avec KN
306
E2{KN}(X)
307
X = Kc XOR K'c
308
Mémorisation X et E2{KN}(X) à la place de Kc et E2{KN}(Kc)
309
...
E2{KN}(X) | E3{X}(CW) | E4{CW}(<Données>)
310
t
t

Fig. 4

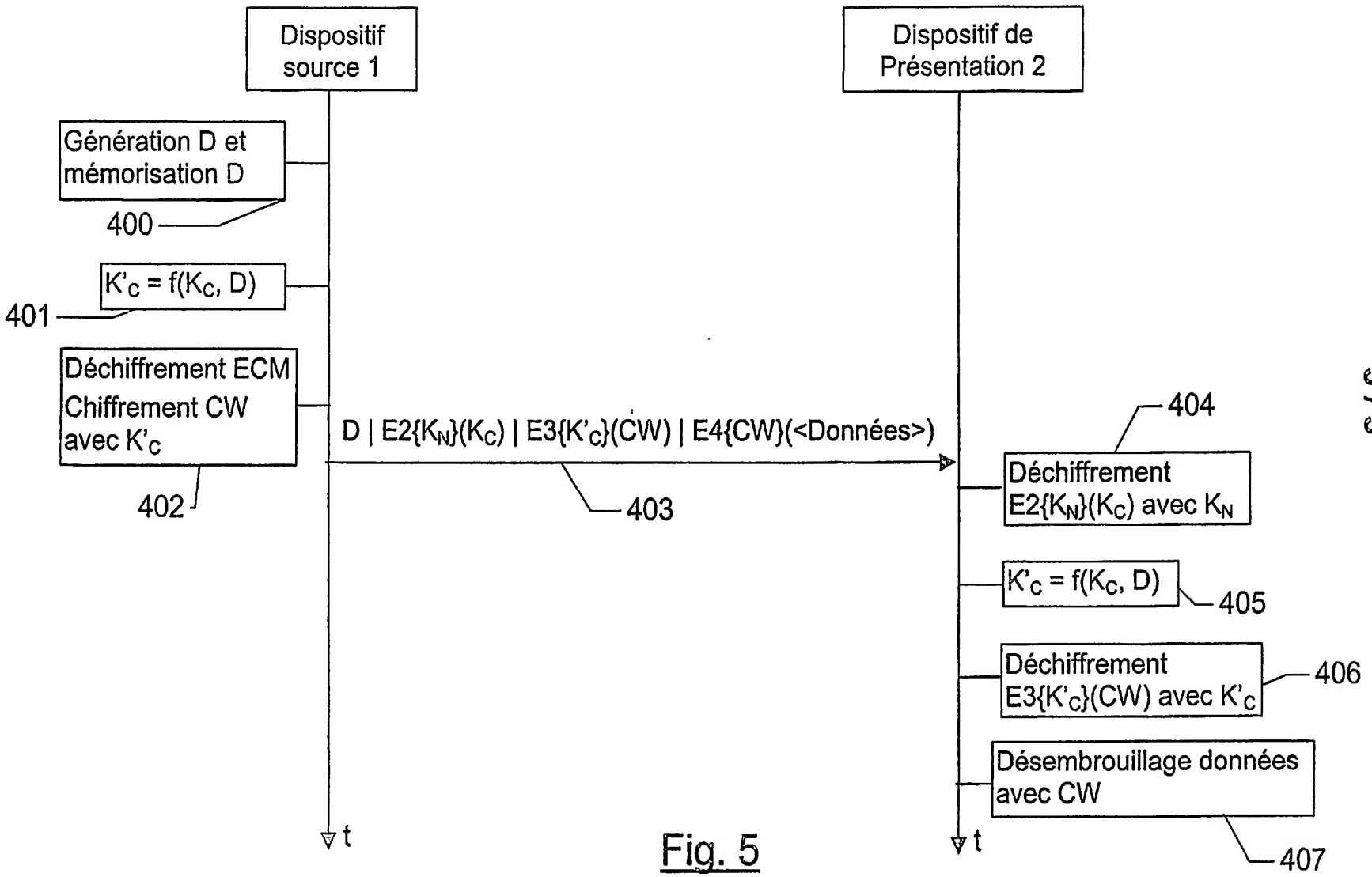

Dispositif source 1
Dispositif de Présentation 2
Génération D et mémorisation D
400
K'C = f(KC, D)
401
Déchiffrement ECM
Chiffrement CW avec K'C
402
D | E2{KN}(KC) | E3{K'C}(CW) | E4{CW}(<Données>)
403
404
Déchiffrement E2{KN}(KC) avec KN
K'C = f(KC, D)
405
Déchiffrement E3{K'C}(CW) avec K'C
406
Désembrouillage données avec CW
407
t
t

Fig. 5

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 G VI / 270601

Vos références pour ce dossier *(facultatif)*	PF020148
N° D'ENREGISTREMENT NATIONAL	02/13982

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE GESTION DE CLES SYMETRIQUES DANS UN RESEAU NUMERIQUE

LE(S) DEMANDEUR(S) :

THOMSON LICENSING SA
46 Quai Alphonse Le Gallo
92648 Boulogne cedex
FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		DURAND
Prénoms		Alain
Adresse	Rue	79, rue de Dinan
	Code postal et ville	35000 Rennes
Société d'appartenance *(facultatif)*		
2 Nom		ANDREAUX
Prénoms		Jean-Pierre
Adresse	Rue	20 rue de Lorgeril
	Code postal et ville	35000 Rennes
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

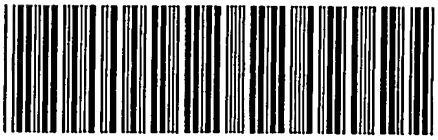
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Martin KOHRS
Mandataire

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PCT Application
FR200303250



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.